Vol.2017-CSEC-79 No.3
2017/12/4

HPKI認証の特長を考慮した在宅医療介護システムにおける患者情報の開示先制御

稲吉 陽一朗[1,a)]　白石 善明[2]　竹尾 淳[1]　加藤 昇平[1]　矢口 隆明[1]　岩田 彰[1]

概要：在宅医療介護連携における多職種の医療介護従事者の間の情報共有に ICT を活用することで，チームケアが円滑となり，サービスの質が向上や効率化に繋がることが期待されている．しかし，そのような情報システムでは患者の機微な個人情報を一元管理する．よって，それらは暗号化保管されることが望ましい．また，保健医療福祉分野では専用の公開鍵基盤（HPKI）が整備されている．そこで，本稿では HPKI による認証によって担保される情報に基づいて，暗号化された個人情報の開示先制御を行う方式を 2 つ提案する．まず，代表的な公開鍵暗号である RSA 暗号によって構成する方式を，次に暗号文ポリシー属性ベース暗号（CP-ABE）によって構成する方式を提案する．また，この 2 方式における暗号化および復号処理時間を測定した．その結果，RSA 方式は変化頻度の大きい情報の開示先制御に，CP-ABE 方式は変化頻度の小さく緊急時に最低限必要となる情報の開示先制御に適していることが分かった．

キーワード：在宅医療介護連携，開示先制御，HPKI，暗号文ポリシー属性ベース暗号

Information Disclosing Mechanism Using a Feature of the Healthcare PKI for Collaboration of Home Medical Care and Nursing Services

Yoichiro INAYOSHI[1,a)]　Yoshiaki SHIRAISHI[2]　Jun TAKEO[1]　Shohei KATO[1]
Takaaki YAGUCHI[1]　Akira IWATA[1]

Abstract: In home medical care and nursing, information sharing using ICT among medical care workers makes team care smooth and improves quality and efficiency of medical care and nursing care. However, in such a system, sensitive personal information of patients should be encrypted and stored, because it is exchanged through the internet. In addition, there is dedicated public key infrastructure (HPKI) in the health and welfare field. Therefore, we show two methods of information disclosing mechanism based on the HPKI. One is a RSA method using RSA. The other is a CP-ABE method using Ciphertext-Policy Attribute-Based Encryption. We measured processing time of encryption and decryption in those two methods. The results showed that RSA method is suitable for disclosing mechanism of information with high change frequency, and CP-ABE method is suitable for some with low change frequency.

Keywords: Collaboration of Home Medical Care and Nursing, Disclosure Control, Healthcare Public Key Infrastructure, Ciphertext-Policy Attribute-Based Encryption

1. はじめに

在宅医療介護においては，一人の在宅患者に対し，多機関多職種の医療介護従事者が一体となってサービスを提供するチームケアが求められている．また，ICT 利活用に関する調査 [1] では，在宅医療介護において医療介護従事者

[1] 名古屋工業大学
Nagoya Institute of Technology, Gokiso-cho, Shouwaku, Nagoya-shi, Aichi, 466–8555, Japan
[2] 神戸大学
Kobe University, Rokkodai-cho 1–1, Nadaku, Kobe-shi, Hyogo, 657–8501, Japan
[a)] inayoshi@katolab.nitech.ac.jp

間の情報共有に ICT を活用することでチームケアが円滑となり，医療・介護の質の向上や効率化が期待されることが示されている．

しかし，在宅医療介護連携のための情報共有システムでは患者の医療情報という機微な情報 [2] をはじめ，患者の生活状況や家族に関する情報などのプライバシー性の高い個人情報を扱う．したがって，その開示先はケアチームのメンバーに厳密に限定されなければならない．また，今後より多くの個人情報がサーバに電子化保存されることを想定すると，外部からの攻撃によるサーバからの情報漏洩の危険性がある．これに対して，個人情報の暗号化保管により，漏洩時に直ちにその内容が明らかになるリスクを低減することができる．すなわち，在宅医療介護連携システムにおいては，暗号化保管された個人情報の開示先制御が必要となる．

また，保健医療福祉分野では，利用者のなりすましや情報の改竄を防ぐために，専用の公開鍵基盤（Healthcare Public Key Infrastructure: HPKI）が整備されている．平成 21 年度には「保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ」[3] の策定が行われ，認証用の HPKI 証明書の発行が行えることとなった．

個人情報の厳密な開示先制御を考える上では，開示先の正当性を確認する認証を合わせて考える必要がある．しかし，関連研究ではその点について考慮されていない [4]．そこで，本稿では HPKI による認証によって担保される情報に基づいて，暗号化された個人情報の開示先制御を行う方式を 2 つ提案する．まず，代表的な公開鍵暗号である RSA 暗号によって構成する方式と，次に属性ベース暗号の一種である暗号文ポリシー属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption: CP-ABE）によって構成する方式を提案する．また，暗号化および復号処理時間の測定により，2 方式を評価する．

2. 暗号文ポリシー属性ベース暗号（CP-ABE）

CP-ABE は Bethencourt[5] らによって提案されており，以下の 4 つのアルゴリズムからなる．

Setup セキュリティパラメータ λ を入力として，マスタ公開鍵 PK とマスタ秘密鍵 MK を出力する．

Encrypto マスタ公開鍵 PK と平文 M，またアクセス構造 P を入力として，暗号文 CT を出力する．

Keygen マスタ秘密鍵 MK とユーザの属性集合 S を入力として，秘密鍵 SK を出力する．

Decrypto マスタ公開鍵 PK と秘密鍵 SK，暗号文 CT を入力として，SK の属性集合 S が CT のアクセス構造 P を満たす場合，平文 M を出力する．

PKG(Private Key Generater) と呼ばれる信頼された機関が Setup においてマスタ公開鍵とマスタ秘密鍵の生成し，そのうちマスタ公開鍵をユーザに配布し，マスタ秘密鍵をセキュアに管理する．また，PKG は Keygen においてマスタ秘密鍵を用いてユーザの属性集合に対応した秘密鍵を生成し発行する．また，Encrypto において暗号文に埋め込むアクセス構造は，職種や所属等の属性を論理式の形で表現される．例えば，“人事部 and （部長 or 課長）” である．これを満たす属性集合に対応した秘密鍵のみ，暗号文を復号可能となる．

表 1 hcRole 属性として記載可能である資格名 [3]

資格名（国家資格）	説明
‘Medical Doctor’	医師
‘Dentist’	歯科医師
‘Pharmacist’	薬剤師
‘Medical Technologist’	臨床検査技師
‘Radiological Technologist’	診療放射線技師
‘Registered Nurse’	看護師
‘Public Health Nurse’	保健師
‘Midwife’	助産師
‘Physical Therapist’	理学療法士
‘Occupational Therapist’	作業療法士
‘Orthoptist’	視能訓練士
‘Speech Therapist’	言語聴覚士
‘Dental Technician’	歯科技工士
‘National Registered ‘Dietitian’	管理栄養士
‘Certified Social Worker’	社会福祉士
‘Certified Care Worker’	介護福祉士
‘Emergency Medical Technician’	救急救命士
‘Psychiatric Social Worker’	精神保健福祉士
‘Clinical Engineer’	臨床工学技士
‘Massage and Finger Pressure Practitioner’	あん摩マッサージ指圧師
‘Acupuncturist’	はり師
‘Moxibustion Practitioner’	きゅう師
‘Dental Hygienist’	歯科衛生士
‘Prosthetics & Orthctic’	義肢装具士
‘Artificial Limb Fitter’	柔道整復師
‘Clinical Laboratory Technician’	衛生検査技師

3. HPKI による認証

HPKI による認証の概要を説明する．なお，現在 HPKI においては署名用証明書ポリシと認証用証明書ポリシが策定されているが，ここでは単に証明書と記述した場合，認証用証明書を指すこととする．HPKI による電子認証の仕組み自体は，PKI 認証と同様であり，認証用の秘密鍵と公開鍵証明書を用いる．秘密鍵による署名の検証により本人性を確認し，公開鍵証明書の検証により実在性を確認することで証明書所有者を認証する．そして，システムやアプリケーションでは証明書に記載された情報に基づいて加入者を識別し，与えられた権限を確認することで，情報へのアクセスに対する許可を行う [6]．

証明書の基本領域に記載される Subject(加入者名) 内の

表 2　疾患・職種別情報発信件数の割合（%）[7]

疾患 / 職種	がん	認知症	心疾患	肺疾患	骨折
医師	39.4	14.5	17.4	13.3	11.4
歯科医師	0.0	5.1	6.7	15.6	9.3
薬剤師	6.4	0.2	1.2	0.0	5.5
看護師	41.8	18.1	21.4	37.8	18.1
介護支援専門員	5.8	16.1	17.4	33.3	26.2
理学療法士	5.5	4.2	15.9	0.0	8.4
歯科衛生士	0.3	3.2	7.0	0.0	15.2
介護職	0.9	38.6	13.0	0.0	5.9

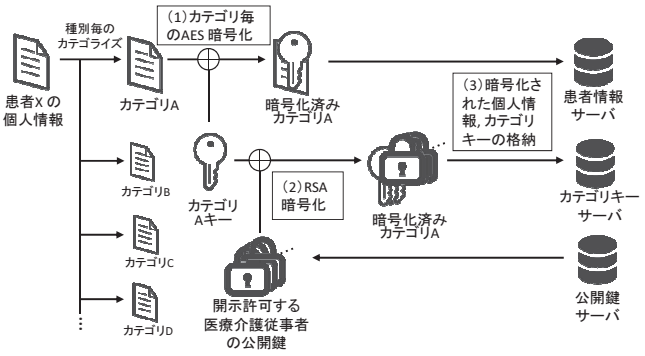

図 1　個人情報の暗号化（RSA 方式）

シリアル番号には，加入者に一意な番号を含むことができる．この場合，このシリアル番号によって，加入者を一意に識別することができる．

また，拡張領域には hcRole 属性という ISO 17090 で規定される国家資格（表 1）や医療機関の管理責任者の資格情報が記載される [3]．この hcRole 属性により加入者の国家資格情報を確認できることは HPKI 認証用証明書の特長のひとつである．

4. 在宅医療介護連携における情報共有

文献 [7] では，既に在宅医療と介護の医療介護従事者が ICT により情報共有をしている先進地域で交わされた文章・単語を調査分析している．調査対象データは，対象地域の患者毎にチーム化された医療介護従事者が，177 人の患者について実際に交わされた 1 年間分の文章データ 6342 件である．表 2 に，種類の疾患「がん」「認知症」「心疾患」「肺疾患」「骨折」の患者別に，交わされた文章の総数に対する各職種の情報発信件数の割合 (%) を示す．「がん」の患者に対しては，看護師 (41.8%) と医師 (39.4%) で全体の 81.2%を占めている一方，「肺疾患」の患者に対しては，看護師 (37.8%) と介護支援専門員 (33.3%) で全体の 71.1%を占めている．このように患者の疾患の種類により，職種毎の関わり方は異なることが分かっている．また，介護支援専門員について，現状では，hcRole 属性（表 1）に含まれていない．しかし，ここで分かるように，介護支援専門員は看護師に次いで情報発信している．よって，本稿では，hcRole 属性に介護支援専門員を追加考慮する．

5. 提案方式

5.1 概要

提案方式では，患者の個人情報自体の暗号化は，公開鍵暗号に比べ処理が高速な共通鍵暗号で行い，AES を利用する．また，厚生労働省による医療情報システムに関するガイドライン [8] に則り，開示する個人情報の範囲を制御するため，患者の個人情報を基本属性や家族，医療，介護 [9] などの種別毎にカテゴライズする．そして，カテゴリ毎に固有のカテゴリキー（AES 鍵）を生成し，それによって暗号化する．また，開示先単位に公開鍵暗号の鍵を生成し，その鍵によってカテゴリキーの配送，管理を行うことで，個人情報をカテゴリ毎に開示先制御を行う．これらの手順は，患者主導型の開示先制御に関する研究 [10] における暗号化保管された情報の開示先制御を参考にしている．本研究では，開示先単位に生成する鍵における公開鍵暗号に代表的である RSA を利用する方式と，CP-ABE を利用する方式を提案する．なお，以降，本稿ではこの 2 方式をそれぞれ RSA 方式と CP-ABE 方式と表記する．

5.2 RSA 方式

RSA 方式では，あらかじめ開示先単位に RSA 公開鍵ペアを生成する．生成した RSA 公開鍵ペアのうち，公開鍵は公開鍵サーバで，秘密鍵は秘密鍵サーバで保管する．

ここで，RSA 公開鍵ペアを生成する対象に関して，HPKI による認証によって担保される情報の利用を考慮すると，医療介護従事者単位の場合に加え，hcRole 属性の利用により職種単位の場合が考えられる．しかし，上で述べたように，在宅医療介護では，患者の疾患の種類によって，職種毎に患者への関わり方が異なっていることが明らかになっているため，職種単位の開示先制御においては，各医療介護従事者を担当している患者と紐付け，その上で職種単位の開示先制御を行うことが適切であると考えられる．よって，職種単位に RSA 公開鍵ペアを生成する際は，患者毎の職種単位に生成する必要がある．したがって，RSA 公開鍵ペアを医療従事者単位に生成する場合，その総数は医療介護従事者の総数となり，職種単位に生成する場合，その総数は患者の数 × 患者に関わる職種数となる．この 2 つの場合において生成される RSA 公開鍵ペアの総数について，統計データに基づき算出したところ，医療介護従事者単位に生成する場合の方がその数が小さいことが分かっている [11]．よって，鍵管理コストの観点から，ここでは医療介護従事者単位に RSA 公開鍵ペアと ID を生成し，それらを紐付けて開示先制御を行う．以下に，この方式における個人情報の暗号化と復号，また開示先の追加・削除について説明する．

個人情報の暗号化

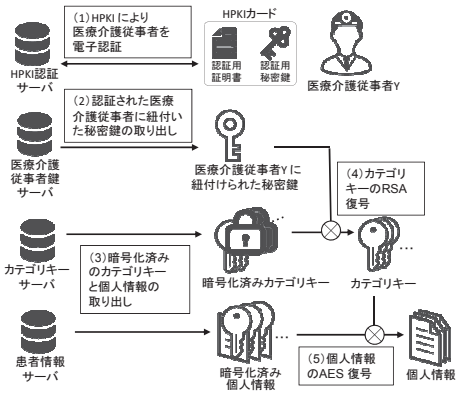

図 2 個人情報の復号（RSA 方式）

患者の個人情報を暗号化する手順は図 1 のようになる．なお，図 1 は，ある患者 X の個人情報の一つのカテゴリ A の暗号化手順を示している．

(1) 種別毎にカテゴライズされた個人情報をカテゴリ毎に生成したカテゴリキーで AES 暗号化する
(2) 開示許可する医療介護従事者の公開鍵を公開鍵サーバから取り出し，その公開鍵でカテゴリキーを RSA 暗号化する
(3) 暗号化された，個人情報とカテゴリキーをそれぞれのサーバに格納する

個人情報の復号

医療介護従事者が HPKI による認証を経て，患者の個人情報を復号する手順は図 2 のようになる．なお，図 2 は，ある医療従事者 Y が個人情報を復号する手順を示している．

(1) HPKI により医療介護従事者を電子認証する
(2) 医療介護従事者鍵サーバから，認証された医療介護従事者の ID に紐付けられた秘密鍵を取り出す
(3) 取り出した秘密鍵に対応する公開鍵によって暗号化されているカテゴリキーと，そのカテゴリキーによって暗号化されている個人情報をそれぞれ，カテゴリキーサーバと個人情報サーバから取り出す
(4) 秘密鍵でカテゴリキーを RSA 復号する
(5) カテゴリキーで個人情報を AES 復号する

開示先の追加・削除

患者の個人情報の開示先の追加の手順は図 3 のようになる．図 3 は，ある医療介護従事者 Y が個人情報の一つのカテゴリ A の開示先を追加する手順を示している．なお，開示先の追加については，既に開示許可されているものが行うこととする．

(1) HPKI により医療介護従事者を電子認証する
(2) 医療介護従事者鍵サーバから，認証された医療介護従事者の ID に紐付けられた秘密鍵を取り出す
(3) 取り出した秘密鍵に対応する公開鍵によって暗号化されているカテゴリキーと，そのカテゴリキーによって暗号化されている個人情報をそれぞれ，カテゴリキーサーバと個人情報サーバから取り出す
(4) 秘密鍵でカテゴリキーを RSA 復号する
(5) 開示先として追加したい医療介護従事者の ID に紐付いた公開鍵を公開鍵サーバから取り出し，その公開鍵でカテゴリキーを RSA 暗号化する
(6) 暗号化したカテゴリキーをカテゴリキーサーバに格納する

また，既に開示先として追加されている医療介護従事者を開示先から削除する場合には，その ID に紐付いた公開鍵によって暗号化されているカテゴリキーをカテゴリキーサーバから削除するだけでよい．

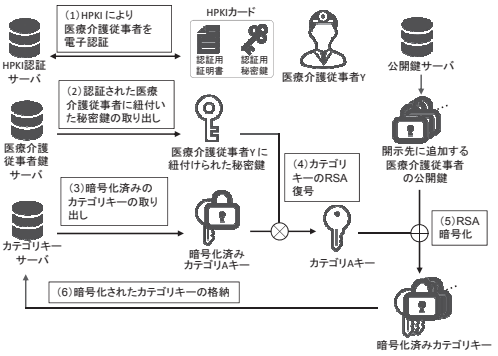

図 3 開示先の追加（RSA 方式）

5.2.1 RSA 方式の欠点

災害時や患者の容態の急変時などには，普段はその患者に関わっていないケアチーム外の医療介護従事者であっても，いち早くその患者の情報を把握し最適な対応をする必要がある．そのため，患者の状況に応じた個人情報の開示先制御が重要である [12]．hcRole 属性を開示先制御に利用することは加入者を一意に特定する必要がないため，緊急時における専門資格を持つ加入者への個人情報の開示許可等の利用場面に有用である [6]．しかし，RSA 方式では，医療介護従事者はあらかじめ自身に紐付けられた公開鍵によって暗号化した情報しか復号できないため，このような HPKI の特長を活かした開示先制御ができていない．また，医療介護従事者毎に生成した RSA 公開鍵ペアにおける秘密鍵はセキュアに管理されなければならなく，システムを運用していく上で考慮すべきコストとなる．

5.3 CP-ABE 方式

CP-ABE 方式でも，あらかじめ各医療介護従事者に ID を生成しておく．そして，カテゴリキーを CP-ABE で暗号化する．例えば，開示したい医療介護従事者が 2 人とし，それぞれの ID が 330001，330054 であるとする．その場合，暗号文に埋め込む復号ポリシを “(ID =330001) or (ID =330054)” というように ID を OR で結合する形で記述する．また，システム内で患者の緊急時状態を何らかの属性

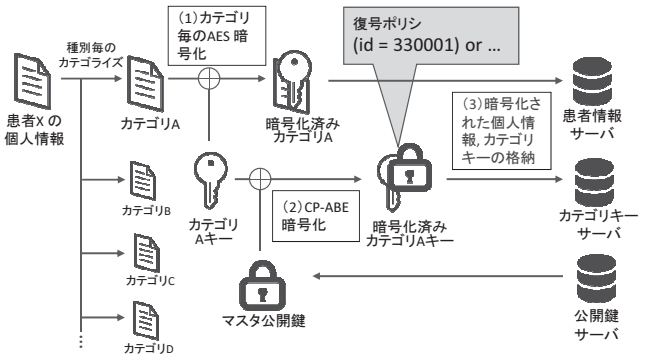

図 4　個人情報の暗号化（CP-ABE 方式）

で表すことができ，これを emergency と表したとする．その場合，hcRole 属性を利用し，例えば，“emergency and Medical_Doctor” を OR 結合することで，開示許可されていない医師であっても，緊急時には医師の国家資格を持つものには情報を開示可能とする緊急時用の復号ポリシを記述することができる．

また，医療介護従事者が HPKI によって認証された場合，その ID と証明書内の hcRole 属性を属性値として埋め込まれた秘密鍵を PKG が生成する．その秘密鍵によって，対応している属性集合が満たす復号ポリシが埋め込まれているカテゴリキーを復号することができる．また，医療介護従事者がシステムからログアウトした際に秘密鍵を削除することで，秘密鍵を管理する必要がなくなる．

以下に，この方式における個人情報の暗号化と復号，また開示先の追加・削除について説明する．なお，以下に示す各手順において，RSA 方式と同様である部分に関しては “RSA 方式と同様” とする．

個人情報の暗号化

患者の個人情報を暗号化する手順は図 4 のようになる．なお，図 4 は，ある患者 X の個人情報の一つのカテゴリ A の暗号化手順を示している．

(1) RSA 方式と同様
(2) マスタ公開鍵を公開鍵サーバから取り出し，開示先許可する医療介護従事者の ID を OR 結合した復号ポリシでカテゴリキーを CP-ABE 暗号化する
(3) RSA 方式と同様

個人情報の復号

医療介護従事者が HPKI による認証を経て，患者の個人情報を復号する手順は図 5 のようになる．なお，図 5 は，ある医師 Z が個人情報を復号する手順を示している．

(1) RSA 方式と同様
(2) PKG が認証された医療介護従事者の ID と証明書内の hcRole 属性に対応した秘密鍵を生成する
(3) RSA 方式と同様
(4) (2) で生成した秘密鍵でカテゴリキーを CP-ABE 復号する
(5) RSA 方式と同様

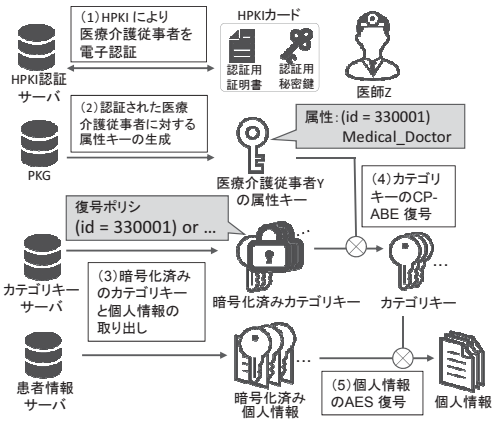

図 5　個人情報の復号（CP-ABE 方式）

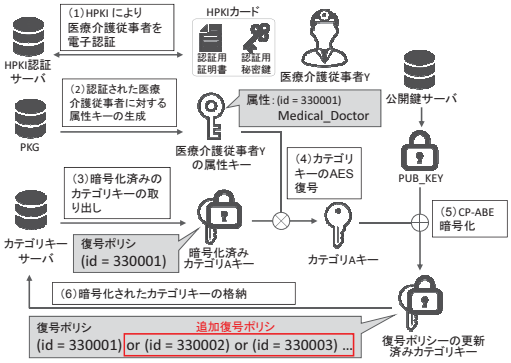

図 6　開示先の追加（CP-ABE 方式）

開示先の追加，削除

患者の個人情報の開示先の追加の手順は図 6 のようになる．図 6 は，ある医師 Z が個人情報の一つのカテゴリ A の開示先を追加する手順を示している．なお，開示先の追加については，既に開示許可されているものが行うこととする．

(1) RSA 方式と同様
(2) PKG が認証された医療介護従事者の ID と証明書内の hcRole 属性に対応した秘密鍵を生成する
(3) RSA 方式と同様
(4) (2) で生成した秘密鍵でカテゴリキーを CP-ABE 復号する
(5) マスタ公開鍵を公開鍵サーバから取り出し，開示先として追加したい医療介護従事者の ID を OR 結合に追加して復号ポリシを更新し，カテゴリキーを CP-ABE 暗号化する
(6) RSA 方式と同様

また，既に開示許可されている医療介護従事者を開示先から削除する場合は，(5) において，その医療介護従事者の ID の OR 結合を削除して復号ポリシを更新し，カテゴリキーを CP-ABE 暗号化する．

表 3　標準的な共有情報 [9]

大項目名	中項目数	小項目数	変化頻度毎の小項目数		
			大	中	小
患者属性	13	32	0	0	32
住居・家族	6	23	0	0	23
医療	16	59	0	29	30
介護・生活	9	71	0	71	0
診療・ケア	8	51	22	29	0

6. RSA 方式と CP-ABE 方式の処理時間の測定

提案方式では，一般的な情報共有システムに要する処理に加え，暗号化や復号の処理を要する．よって，それらの処理時間が許容範囲内であるかどうかを確認する為に各方式における個人情報の暗号化と復号の手順に要する処理の時間を測定した．これらの処理は，クライアントの代わりに演算サーバが実行することとし，測定には，OS が Ubuntu 14.04.5 LTS(64bit)，CPU が Intel®Core™i7-6950X CPU @ 3.00GHz，メモリが 64GB のサーバを利用した．また，各測定は 100 回試行の平均値をとっている．

CP-ABE の処理測定には，Bethencourt[5] らが開発した C 言語のオープンソースのライブラリ Ciphertext-Policy Attribute-Based Encryption を利用する．このライブラリは，(k, n) 閾値秘密分散法によって CP-ABE における復号ポリシの論理演算を実現している．属性数を n とした場合，秘密情報を n 個に分散し，それらを各属性に対応付けた鍵で暗号化する．これらの属性の AND 結合を行う場合，復号に必要な分散情報の数 $k = n$ となり，OR 結合を行う場合，$k = 1$ となる．また，このライブラリでファイルを暗号化する際は，ファイル自体は AES (鍵長 128bit, CBC モード) で暗号化し，AES 鍵を CP-ABE で暗号化しているが，これには，オープンソースライブラリ OpenSSL の AES 暗号化関数を利用している．また，CP-ABE で利用しているペアリング演算ライブラリ内では，RSA（鍵長 2048bit） と同等の暗号強度となるパラメータを設定している．

よって，RSA の処理測定には，OpenSSL を利用して，これに合わせたハイブリッド型の処理を行うプログラムを実装し，利用した．

また，文献 [9] では，在宅医療介護連携における標準的な共有情報を示しており，それらを 5 つの大項目に分類分けし，さらにそれを中項目，小項目で分けている（表 3）．また，情報の最小単位である小項目は，変化頻度が大中小の 3 段階に分けられている．例えば，バイタル情報のように患者の状態によって頻繁に変化する情報は変化頻度が大である．一方で，氏名や住所，かかりつけ医に関する情報などは変化頻度が小とされている．変化頻度は，患者属性や住居・家族が小さく，介護・生活や診療・ケアが大きいことが分かる．

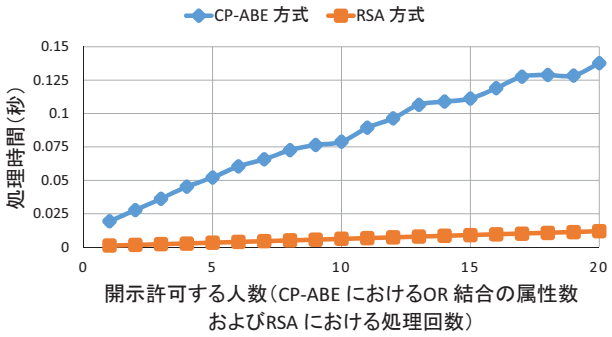

図 7　1 カテゴリ暗号化処理時間

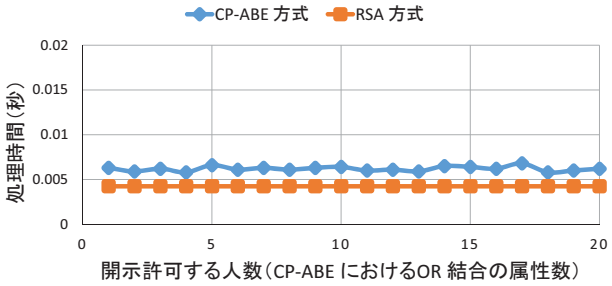

図 8　1 カテゴリ復号処理時間

測定に際しては，小項目をまとめた中項目を提案手法における 1 カテゴリとした．また，1 カテゴリを最大 512 文字と見積もり，測定における暗号化対象ファイルは 1 KB のテキストファイルとした．このとき，AES による暗号化および復号処理時間は RSA および CP-ABE に比べ十分小さく，無視することができる．

復号ポリシに記述する OR 結合の属性数を変化させて測定を行った．暗号化処理に関しては，CP-ABE 方式において，この属性数 = 開示許可する医療介護従事者の数となり，また，この数は RSA 方式における RSA 暗号化処理の繰り返し回数となるため，2 方式の処理時間を同一 2 次元グラフに表すことが可能である．その結果を図 7 に示す．結果としては，開示先人数が大きくなることで，CP-ABE 方式および RSA 方式ともに暗号化回数が大きくなるため，処理時間は大きくなるが，その傾きは RSA 方式に比べ，CP-ABE 方式が大きく，その差は大きくなっていく結果となった．

また，復号処理時間の測定結果を図 8 に示す．RSA 方式においては，復号対象の開示許可人数の影響は受けないため，1 カテゴリの復号処理時間は一定で 0.004 秒 であった．CP-ABE 方式においては，復号対象の開示許可人数が大きくなることで，復号ポリシの属性数が大きくなる．しかし，提案方式においては OR 結合のみの復号ポリシとなるため，1 回の復号処理で復号ポリシを満たすため，処理時間は一定となる．その大きさは平均で 0.006 秒 であり，RSA 復号処理時間と同等であることが分かった．

また，CP-ABE 方式においては，HPKI による認証後，

ID と hcRole 属性に対応する属性キーの生成処理を行うが，そのタイミングは復号処理と異なるため，ここでは考慮していない．また，その処理時間の測定結果は 0.219 秒であり，運用上は問題ないと考えられる．

7. システムの実運用を想定した処理時間に関する考察

実際に医療介護従事者がシステムを利用する際，表 3 における大項目毎に，情報をまとめて閲覧，登録する．この場合，1 度で最大 16 カテゴリ（医療情報）の暗号化および復号処理が必要となる．ここで，文献 [7] の調査研究に合わせ，医師，歯科医師，薬剤師，看護師，介護支援専門員，理学療法士，歯科衛生士，介護福祉士の 8 職種によるケアチームを想定する．また，看護師と介護福祉士は 3 名ずつ（その他の職種は 1 名ずつ）とし，人数は計 12 名と想定する．

復号処理に関しては，1 カテゴリあたりの処理時間が 0.006 秒であるので，16 カテゴリでも 0.096 秒程度と高速で処理することができる．また，例えば，患者のバイタル情報は，測定の度にデータが蓄積していく．このような情報は，過去のデータを複数復号し，時系列上に並べて閲覧する場合がある．1 秒程度で復号することができるデータの数は $1 \div 0.006 \simeq 166.7$ より，166 である．これは測定回数が週に 3 回以下であれば，1 年間分のデータとなるため，運用上大きな問題はないと考えられる．

暗号化処理に関しては，開示許可人数が 12 名のときの 1 カテゴリあたりの処理時間は，0.096 秒 であった．よって，16 カテゴリでは 1.536 秒程度であるので，このケアチームの想定では，暗号化処理に関しても運用上致命的な問題はないと考えられる．しかし，暗号化処理に関しては，緊急時用の復号ポリシを記述することや，より大人数のケアチームになる可能性を考慮すると，システムのレスポンスタイムにおいて，CP-ABE の処理時間が支配的になる可能性がある．よって，患者の個人情報のうち，特に頻繁にシステムへの登録を必要とする，変化頻度の大きい情報を CP-ABE 暗号化するのは適切ではなく，処理が高速な RSA 方式が適している．一方で，変化頻度が小さい情報に関しては，基本的に初回登録の際にしか暗号化処理を必要としないため，処理時間が大きい場合でも運用への影響が小さい．加えて，これらの情報には，患者属性やかかりつけ医，既病歴などが含まれ，緊急時には把握すべき情報が多いため，CP-ABE 方式が適していると考えられる．

8. おわりに

本稿では，在宅医療介護連携システムにおける HPKI による認証を想定し，これによって担保される情報に基づいた患者の個人情報の開示先制御を RSA 暗号によって構成する方式と，CP-ABE によって構成する方式を提案した．また，2 方式における個人情報の暗号化と復号処理の手順に要する処理時間を測定した．その結果，処理時間としては，暗号化，復号ともに RSA 方式が高速であった．CP-ABE 方式においても，運用上問題ない速度で復号処理が可能であることが分かった．しかし，暗号化処理に関しては，緊急時用の復号ポリシや大人数のチームケアにより，システムのレスポンスタイムにおいて，処理時間が支配的になる可能性がある．よって，RSA 方式は変化頻度の大きい情報の開示先制御に，また，CP-ABE 方式は変化頻度の小さく，緊急時に重要な情報の開示先制御に適していると考えられる．しかし，この 2 方式の併用では，CP-ABE 方式における各医療介護従事者に対応する秘密鍵の管理の低減という利点の効果がなくなってしまう．

よって，今後の課題は変化頻度が大きい情報に対しての CP-ABE 方式の適用方法を考案することが挙げられる．具体的には，現状は復号ポリシの記述方法が医療介護従事者の ID を OR 結合で並べる単純なものであるため，復号ポリシにおける属性数を削減することで暗号化処理の高速化を図る．また，RSA 方式における公開鍵ペアの生成について，本稿では hcRole 属性を利用した職種毎ではなく，より生成数が少ない各医療従事者単位とした．しかし，この場合でも公開鍵ペアに hcRole 属性を紐付けておけば，緊急時にはケアメンバー外の者であっても hcRole 属性を確認した上でそれに一致するメンバー内の者の鍵を利用可能とすれば，緊急時に hcRole 属性を活かした開示先制御を可能である．よって，それを考慮した上での CP-ABE 方式との比較・考察を行うことも挙げられる．

参考文献

[1] 株式会社情報通信総合研究所：地域における ICT 利活用の現状に関する調査研究報告書 (online)，入手先 ⟨http://www.soumu.go.jp/johotsusintokei/linkdata/h27_07_houkoku.pdf⟩，（参照 2017-11-02）．
[2] 経済産業省：JIS Q 15001:2006(online)，入手先 ⟨http://www.meti.go.jp/policy/it_policy/privacy/jis_shian.pdf⟩，（参照 2017-11-02）．
[3] 厚生労働省：保健医療福祉分野 PKI 認証局 認証用（人）証明書ポリシ 1.4 版 (online)，入手先 ⟨http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000112704.pdf⟩，（参照 2017-11-02）．
[4] 立田 太一，溝口 航，白石 善明ほか：在宅医療介護情報連携システムにおける連結可能匿名化とハイブリッド暗号方式を組み合わせたセキュアな個人情報管理手法，信学技報，vol.112，no.466，pp.65-70（2013）
[5] Bethencourt, J., Sahai, A. and Waters, B.: Ciphertext-policy attribute-based encryption, Proc. IEEE Symposium on Security and Privacy, pp.321-334(2007).
[6] 一般社団法人 保険医療福祉情報システム工業会 医療システム部会 セキュリティ委員会：JAHIS HPKI 電子認証ガイドライン V1.1(online)，入手先 ⟨https://www.jahis.jp/files/user/images/JAHIS_HPKI_V1.1.pdf⟩，（参照 2017-11-02）．

[7] 在宅医療と介護の多職種連携に関する調査研究委員会:在宅医療と介護の連携のための情報システムの共通基盤のあり方に関する調査研究報告書(online),入手先 ⟨http://www.iog.u-tokyo.ac.jp/wp-content/uploads/2015/04/01667ff78127f3599d21c25a6906f782.pdf⟩,(参照 2017-11-02).
[8] 厚生労働省:医療情報システムの安全管理に関するガイドライン 第 5 版(online),入手先 ⟨http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf⟩,(参照 2017-11-02).
[9] 在宅医療と介護の連携における情報システム利用に関するガイドライン検討委員会:在宅医療と介護の連携における情報システムの適切な利用を促進するためのガイドライン(草案)(online),入手先 ⟨http://www.iog.u-tokyo.ac.jp/wp-content/uploads/2014/05/5435d2ad3a28ce3767b71b2bfb764856.pdf⟩,(参照 2017-11-02).
[10] Benaloh, J., Chase, M., and Lauter, K., et al. Patient controlled encryption : ensuring privacy of electronic medical records, Proc. ACM CCSW 2009, pp.103-114(2009).
[11] 稲吉 陽一朗,白石 善明,竹尾 淳ほか:HPKI 認証を用いた在宅医療介護連携システムにおける個人情報の開示先制御,信学技報,vol.117,no.199,pp.51-56(2017)
[12] 笠井 敬介,川越 恭二:状況変化を考慮した利用者個人情報のアクセス制御モデルの構築,CSS2009 論文集,pp.1-6(2009)